CLAIMS

What is claimed is:

1. A method, comprising:

receiving, at a first computing device, a request from a second computing device to encrypt a first file resident on the first computing device;

in response to the request,

creating a second file;

copying metadata from the first file to the second file; and

transmitting an identifier associated with the second file to the first computing device.

2. The method of claim 1, wherein the first computing device is a server and the second computing device is a client.

3. The method of claim 1, further comprising:

receiving, at the second computing device, the identifier associated with the second file;

opening the first file and the second file; and

writing header information from the first file to the second file.

4. The method of claim 3, further comprising encrypting the content of the first file.

5. The method of claim 4, further comprising writing the encrypted content to the second file.

6. The method of claim 5, further comprising replacing the first file with the second file.

7. The method of claim 1, wherein creating a second file comprises invoking a file system operation.

8. A computer-readable medium having computer-executable instructions for performing the method recited in claim 1.

9. A method of computing, comprising:

generating, at a first computing device, a request to encrypt a first file;

transmitting the request to a second computing device;

receiving, from the second computing device, an identifier associated with a second file;

opening the first and second files;

writing header information into the second file;

encrypting the contents of the first file;

writing the encrypted contents into the second file; and

replacing the first file with the second file.

10. The method of claim 9, wherein the first computing device is a server and the second computing device is a client.

11. The method of claim 9, further comprising creating, at the second computing device, a second file and copying metadata associated with the first file to the second file.

12. A computer-readable medium having computer-executable instructions for performing the method recited in claim 9.

13. A method of computing, comprising:

generating, at a client computing device, a request to encrypt a first file;

transmitting the request to a server computing device;

in response to the request, at the server computing device,

creating a second file;

copying metadata from the first file to the second file; and

transmitting an identifier associated with the second file to the client computing device;

in response to the receipt of the identifier, at the client computing device,

opening the first and second files;

writing header information into the second file;

encrypting the contents of the first file;

writing the encrypted contents into the second file; and

replacing the first file with the second file.

14. A computer system, comprising:

a display;

a user-input device;

a processor capable of executing logic instructions; and

a computer readable medium comprising logic instructions executable on the processor for:

receiving a request to encrypt a first file resident on a first computing device; and

in response to the request,

creating a second file;

copying metadata from the first file to the second file; and

transmitting an identifier associated with the second file to the first computing device.

15. A method of computing, comprising:

receiving, at a first computing device, a request from a second computing device to decrypt a first file resident on the first computing device;

in response to the request,

creating a second file;

copying metadata from the first file to the second file;

decrypting the first file;

writing contents of the first file to the second file; and

replacing the first file with the second file.

16. The method of claim 15, wherein the first computing device is a server and the second computing device is a client.

17. The method of claim 15, wherein the second computing device obtains the file encryption key from the first computing device and forwards the file encryption key with the request to decrypt a file.

18. The method of claim 17, wherein the second computing device invokes a remote file system operation to obtain the FEK.

19. A computer-readable medium having computer-executable instructions for performing the method recited in claim 15.

20. A method of computing, comprising:

generating, at a first computing device, a request to decrypt a first file;

obtaining the file encryption key of the first file; and

generating a transmission containing the file encryption key for forwarding to a second computing device with the request to decrypt the first file.

21. The method of claim 20, wherein obtaining the file encryption key of the first file comprises obtaining the $EFS stream of the first file and extracting the file encryption key from the $EFS stream.

22. The method of claim 21, wherein obtaining the file encryption key of the first file comprises invoking a remote file system operation.

23. A computer-readable medium having computer-executable instructions for performing the method recited in claim 20.

24. A method of computing, comprising:

generating, at a first computing device, a request to decrypt a first file;

obtaining the file encryption key of the first file; and

forwarding the file encryption key to a second computing device with the request to decrypt the first file;

in response to the request, at the second computing device,

creating a second file;

copying metadata from the first file to the second file;

decrypting the first file;

writing contents of the first file to the second file; and

replacing the first file with the second file.

25. The method of claim 24, wherein obtaining the file encryption key of the first file comprises obtaining the $EFS stream of the first file and extracting the file encryption key from the $EFS stream.

26. The method of claim 24, wherein obtaining the file encryption key of the first file comprises invoking a remote file system operation.

27. A computer system, comprising:

a display;

a user-input device;

a processor capable of executing logic instructions; and

a computer readable medium comprising logic instructions for:

receiving a request from a second computing device to decrypt a first file resident on a first computing device;

creating a second file;

copying metadata from the first file to the second file;

decrypting the first file;

writing contents of the first file to the second file; and

replacing the first file with the second file.

28. A method of adding a user to an encrypted file stored on a server, comprising:

obtaining the $EFS stream of the encrypted file from the server;

generating a DDF for the user;

modifying the $EFS stream to include the DDF for the user; and

writing the $EFS stream to the server.

29. The method of claim 28, wherein obtaining the $EFS stream from the server comprises invoking a remote procedure call.

30. The method of claim 28, wherein writing the $EFS stream to the server comprises invoking a remote procedure call.

31. A method of removing a user from an encrypted file stored on a server, comprising:

obtaining the $EFS stream of the encrypted file from the server;

locating a DDF corresponding to the user in the $EFS stream;

modifying the $EFS stream to include the DDF for the user; and

writing the $EFS stream to the server.

32. The method of claim 31, wherein obtaining the $EFS stream from the server comprises invoking a remote procedure call.

33. The method of claim 31, wherein writing the $EFS stream to the server comprises invoking a remote procedure call.

34. A computer system, comprising:

at least one processor;

at least one computer readable medium communicatively connected to the processor and comprising at least one file system component adapted to execute on the one or more processors, wherein the at least one file system component configures the at least one processor to:

access encrypted data that resides on a remote computing device; and

provide the encrypted data to a requesting application in a decrypted format.

35. The system of claim 34, wherein the remote computing device comprises a server in a client-server computer network.

36. The system of claim 34, wherein the remote computer device comprises a client in a peer-peer computer network.

37. The system of claim 34, wherein the remote computer device comprises a client configured to establish a connection with itself as a multi-user system.

38. The system of claim 34, wherein the at least one processor is configured to access encrypted data using the SMB protocol.

39. A method of providing proof that a first computing device possesses a key for decrypting a file associated with a second computing device, comprising:

at a first computing device:

using a unique data stream as a nonce;

determining a hash of the unique data stream;

generating a signature of the hash; and

transmitting, to the second computing device, the signature of the hash and a certificate associated with the key; and

at the second computing device:

verifying the signature of the hash; and

comparing the received hash to a hash list associated with a second computing device.

40. The method of claim 39, wherein the unique data stream comprises an $EFS stream associated with the file.